Virtual Private Network – Einsatzvarianten an der HU

Thomas Gleißner | Thomas.Gleissner@cms.hu-berlin.de

Der folgende Artikel richtet sich an die Benutzer, die sich mit nicht öffentlichen Ressourcen des Netzes der HU verbinden wollen. Momentan werden hierzu an der Humboldt Universität verschiedene VPN-Zugangsverfahren angeboten, die es den Benutzern ermöglichen, sich mit dem Netz der HU zu verbinden. Nachfolgend werden diese Varianten der VPN-Zugänge vorgestellt.

Was versteht man unter einem VPN und wozu dient es?

VPN steht für „Virtual Private Network". Hierunter versteht man ein Netzwerk, in dem einrichtungsinterne Daten mit Hilfe einer sicheren verschlüsselten Punkt-zu-Punkt-Verbindung (VPN-Tunnel) über unsichere Netze, wie das Internet, transportiert werden. Ein äußerer Rechner wird somit Bestandteil des HU-Netzes, d. h. mittels VPN ist man somit in der Lage, die internen Dienste der HU zu nutzen. Das sind z. B.:

- Zugriffe auf Netzlaufwerke der Institute und Einrichtungen
- Online-Inhalte der Universitätsbibliothek
- Nutzung des SMTP-Server zum Versenden von E-Mails

Aus diesem Grund bietet die HU den Angehörigen der Universität die Möglichkeit, sich mit ihrem PC von außen oder auch aus dem internen WLAN in das Netz der Humboldt-Universität einzuwählen. Voraussetzung für die Benutzung eines VPN-Zugangs ist ein gültiger Account in einer der nachstehenden Einrichtungen:

- Computer- und Medienservice
- Institut für Informatik
- Institut für Physik
- Institut für Mathematik
- Universitätsverwaltung

Folgende VPN-Zugangsvarianten werden derzeit vom CMS angeboten:

1. SSL-VPN-Gateway

Herkömmliche IPSec (Internet Protokoll Security) – VPNs, z. B. Cisco VPN, bauen einen Tunnel zwischen zwei Endpunkten auf. Da der aufgebaute Tunnel auf Netzebene des OSI-Modells arbeitet, sind hierbei keine Beschränkungen hinsichtlich der Zugriffsrechte möglich, d. h. der Client Rechner, der über den Tunnel zugreift, sieht das gesamte interne Netz. Des Weiteren wird bei IPsec-VPNs ein jeweils an das Betriebssystem angepasster Client benötigt.

Durch die wachsende Verbreitung von netzwerkfähigen PDAs und ähnlichen mobilen Kleingeräten hat sich der CMS daher entschlossen, VPN-SSL (Secure Sockets Layer) einzusetzen. Hierbei dient ein VPN-SSL-Gateway der Firma Juniper als Zugang für webbasierte Anwendungen. Dieses VPN-Gateway ist unter der Adresse *http://ssl.cms.hu-berlin.de* zu erreichen.

Der entscheidende Vorteil liegt darin, dass heutzutage in jedem Web-Browser das SSL-Protokoll für einen sicheren Zugriff integriert ist. Dank dieser Integration kann ein webfähiges Gerät, wie z. B. ein Firmen-Laptop, ein Smartphone oder PDA etc. sicher auf die webbasierten Ressourcen der HU zugreifen. Zudem werden durch die von den Browsern hergestellten temporären VPN-Verbindungen die auftretenden Probleme hinsichtlich Firewall oder Network Adress Translation (NAT), wie sie z. B. bei IPsec-Verbindungen bestehen, umgangen.[1] Darüber hinaus benötigt der Benutzer keine Konfigurationsdateien, wie sie bei OpenVPN oder Cisco VPN notwendig sind.

Sollte ein weitergehender Zugriff auf nicht webbasierte Anwendungen notwendig sein, so kann das Java-Applet – Network Connect – als vollwertiger IPSec-Client installiert werden. Voraussetzung dafür sind ein aktueller Browser und eine aktuelle Version der Java-Software sowie Admin-Rechte für die Installation. Durch die Installation von Network Connect können somit auch die lokalen Anwendungen des PCs durch den IPSec-Tunnel auf entfernte Server der HU zugreifen.

2. OpenVPN

Der OpenVPN-Cluster befindet sich derzeit in der Evaluierungsphase. Das bedeutet:

- Es können unangekündigte Störungen auftreten, insbesondere während der Bürozeiten.
- Wir bemühen uns, außerhalb der Bürozeiten einen stabilen Status des Clusters sicherzustellen.
- Der Durchsatz und die Stabilität der VPN-Verbindungen sind nicht garantiert.
- Feedbacks an *vpn@cms.hu-berlin.de* sind willkommen.

Warum OpenVPN?

Aus mehreren Gründen ist ein Einsatz von OpenVPN sinnvoll. OpenVPN ist zurzeit für Linux, Windows und MacOS X (OpenVPN-Client Tunnelblick) verfügbar, wodurch es sich für heterogene Netzwerke anbietet. Dabei wird das anerkannt sichere Verschlüsselungsverfahren – OpenSSL – benutzt. Es ist eine freie Software (Open Source) und kann von jedem kostenlos benutzt werden. [2] Des weiteren ist der Installationsaufwand gering und die Konfiguration meist einfach. OpenVPN benötigt lediglich einen einzigen UDP- oder TCP-Port zum Transport der Daten und ist damit besonders NAT- und Firewall-freundlich.

Wie installiert bzw. konfiguriert man OpenVPN?

Unter der URL *http://www.openvpn.net/index.php/open-source/downloads.html* steht die OpenVPN-Software zum Download für die verschiedenen Betriebssysteme bereit.[3] Derzeit läuft unser OpenVPN-Server mit der Version 2.1_rc21, d. h. als Client wird eine Version ab 2.1.0 empfohlen.

Darüber hinaus werden im Gegensatz zum SSL-VPN hierbei folgende zusätzliche Konfigurationsdateien benötigt, welche zum Download bereitstehen:

hu-berlin.conf	-	Konfigurationsdatei für Linux/ Unix und MacOS X
hu-berlin.ovpn	-	Konfigurationsdatei für Windows
ta. Key	-	Schlüsseldatei für DoS-Schutz
ca.crt	-	Zertifikatsdatei der CA

Für die Clientinstallation unter Windows inkl. der Konfigurationsdateien wurde vom CMS eine angepasste OpenVPN-Installer-Version erstellt, welche unter der URL *http://www.cms.hu-berlin.de/dl/netze/vpn/openvpn* zum Download bereit steht. Grundsätzlich gilt: Die Windowsinstallation der OpenVPN-Clientsoftware muss von einem Benutzer mit administrativen Rechten am lokalen System durchgeführt werden.

3. CISCO-VPN

Cisco-VPN wird im CMS bereits seit 2004 eingesetzt. Clientsoftware wird für die gängigsten Betriebssysteme angeboten. Das Protokoll basiert auf IPsec. Die Entwicklung der Software für neuere Systeme, wie etwa Windows 7, erfolgt nur noch schleppend. So wird z. B. kein Client für Windows-Betriebssyteme auf 64-Bit-Basis angeboten. Die Stabilität der Software ist auch nicht immer zufriedenstellend. Die Anbindung der VPN-Konzentratoren ans Backbone-Netz mit 100 MBit/s ist ebenfalls nicht mehr zeitgemäß.

Fazit

Alle drei VPN-Varianten bieten im Prinzip die gleiche Funktionalität, sie unterscheiden sich lediglich im Konfigurations- und Installationsaufwand. Mittelfristig wird die Cisco-VPN-Variante wegfallen, es sollte nur noch eine der beiden anderen Varianten benutzt werden. Sollten Probleme bei der VPN-Installation auftreten, dann schreiben Sie an *oper@cms.hu-berlin.de* bzw. bei schwerwiegenden Installationsproblemen an *vpn@cms.hu-berlin.de*.

Literatur

[1] Juniper SSL VPN. http://www.juniper.net/us/en/products-services/security/sa-series/#literature

[2] *OpenVPN Howto*. http://wiki.freifunk.net/OpenVPN_Howto

[3] Offizielle OpenVPN Homepage: http://www.openvpn.net/index.php/open-source/documentation.html